

THE GROUP RING OF \mathbb{Q}/\mathbb{Z} AND AN APPLICATION OF A DIVISOR PROBLEM

ALAN K. HAYNES AND KOSUKE HOMMA

ABSTRACT. First we prove some elementary but useful identities in the group ring of \mathbb{Q}/\mathbb{Z} . Our identities have potential applications to several unsolved problems which involve sums of Farey fractions. In this paper we use these identities, together with some analytic number theory and results about divisors in short intervals, to estimate the cardinality of a class of sets of fundamental interest.

1. INTRODUCTION

Let G be the multiplicative group defined by

$$G = \{z^\beta : \beta \in \mathbb{Q}/\mathbb{Z}\},$$

and let $(\mathbb{Z}(G), +, \times)$ denote the group ring of G with coefficients in \mathbb{Z} . Clearly G is just \mathbb{Q}/\mathbb{Z} written multiplicatively, but depending on the context it may be more appropriate to speak either of addition in \mathbb{Q}/\mathbb{Z} or of multiplication in G . The group ring $\mathbb{Z}(G)$ is just the ring of formal polynomials with integer coefficients, evaluated at elements of G .

Questions about $\mathbb{Z}(G)$ arise naturally in several elementary problems in number theory. Two interesting examples are the estimation of powers of exponential sums and the problem of approximation of real numbers by sums of rationals. Furthermore the study of the additive structure of arithmetically interesting groups is a fruitful area which has led to significant recent developments [8]. The purpose of this paper is to establish some basic algebraic results about $\mathbb{Z}(G)$ and then to show how recent techniques for dealing with divisors in intervals ([1],[4],[5]) can be applied to estimate the cardinality of an arithmetically interesting class of subsets of G .

For each $\beta \in \mathbb{Q}/\mathbb{Z}$ we denote the additive order of β by $h(\beta)$. Then for each positive integer Q we define a subset \mathcal{F}_Q of \mathbb{Q}/\mathbb{Z} by

$$\mathcal{F}_Q = \{\beta \in \mathbb{Q}/\mathbb{Z} : h(\beta) \leq Q\}.$$

Clearly the set \mathcal{F}_Q can be identified with the Farey fractions of order Q . For $Q \geq 3$ the set

$$\{z^\beta \in G : \beta \in \mathcal{F}_Q\} \subset G$$

is not closed under multiplication. However it does generate a finite subgroup of G , which we call

$$G_Q = \langle z^\beta : \beta \in \mathcal{F}_Q \rangle.$$

2000 *Mathematics Subject Classification.* 11N25, 11B57.

Key words and phrases. Farey fractions, circle group, divisors.

Research of the first author supported by EPSRC grant EP/F027028/1.

Obviously this definition of G_Q is also valid if $Q < 3$. It is easy to check that

$$(1) \quad G_Q = \{z^\beta : \beta \in \mathbb{Q}/\mathbb{Z}, h(\beta) \mid \text{lcm}\{1, 2, \dots, Q\}\}.$$

The cardinality of G_Q is given by

$$|G_Q| = \sum_{q \mid \text{lcm}\{1, 2, \dots, Q\}} \varphi(q) = \text{lcm}\{1, 2, \dots, Q\} = \exp \left(\sum_{q \leq Q} \Lambda(q) \right),$$

where Λ denotes the von-Mangoldt function. Thus by the Prime Number Theorem there is a positive constant c_1 for which

$$(2) \quad |G_Q| = \exp \left(Q + O \left(Q e^{-c_1 \sqrt{\log Q}} \right) \right).$$

It appears to be a somewhat more difficult problem to estimate the cardinality of the set

$$(3) \quad \overbrace{\mathcal{F}_Q + \dots + \mathcal{F}_Q}^{k\text{-times}}$$

when $k \geq 2$ is a small positive integer. The main result of our paper is the following theorem.

Theorem 1. *With $\delta = 1 - \frac{1 + \log \log 2}{\log 2}$ we have as $Q \rightarrow \infty$ that*

$$|\mathcal{F}_Q + \mathcal{F}_Q| \asymp \frac{Q^4}{(\log Q)^\delta (\log \log Q)^{3/2}}.$$

Theorem 1 will be proved in Section 3. The most technical part of the proof uses results of K. Ford [5] about the distribution of integers whose divisors have certain properties. Results of this type were also used in [1] to study gaps between consecutive Farey fractions. Before we get to our proof of Theorem 1 we will develop some important tools that give us information about the corresponding elements of $\mathbb{Z}(G)$. For each nonnegative integer q we define $F_q \in \mathbb{Z}(G)$ by

$$F_q(z) = \sum_{\substack{\beta \in \mathbb{Q}/\mathbb{Z} \\ h(\beta) = q}} z^\beta = \sum_{\substack{a=1 \\ (a,q)=1}}^q z^{a/q}.$$

For conciseness, from on we will suppress the dependance of F_q upon z . In Section 2 we prove the following general result.

Theorem 2. *Suppose that q and r are positive integers. Let $d = (q, r)$ and let d' be the largest divisor of d which is relatively prime to both q/d and r/d . Then we have that*

$$(4) \quad F_q \times F_r = \varphi(d) \sum_{e \mid d'} c(d', e) F_{qr/de},$$

where

$$c(d', e) = \prod_{\substack{p \mid d' \\ p \nmid e}} \left(1 - \frac{1}{p-1} \right).$$

There are several useful consequence of Theorem 2, some of which are formulated in the following two corollaries.

Corollary 1. *With q, r, d , and d' as in Theorem 2 we have that*

(i) If $d' = 1$ then

$$F_q \times F_r = \varphi(d)F_{qr/d}, \quad \text{and}$$

(ii) If q and r are squarefree then

$$F_q \times F_r = \varphi(d) \sum_{e|d} \left(\prod_{p|e} \frac{p-2}{p-1} \right) F_{qre/d^2}.$$

Corollary 2. *If k is a positive integer then the set*

$$\overbrace{\mathcal{F}_Q + \cdots + \mathcal{F}_Q}^{k\text{-times}}$$

consists of all elements $\beta \in \mathbb{Q}/\mathbb{Z}$ with $h(\beta) = n_1 n_2 \cdots n_k$ for some positive integers $n_1, \dots, n_k \leq Q$ which satisfy $(n_i, n_j) = 1$ for $i \neq j$.

As observed by the referee, we note that it is a simple matter to prove Corollary 2 directly and that it is actually all that we need for our proof of Theorem 1. However there are other applications where the more general Theorem 2 is necessary. In particular, by using the large sieve together with the group ring coefficients which appear in our theorem we have been able to give a new proof [7] of an upper bound in metric number theory which is crucial in the classical theory of the Duffin-Schaeffer Conjecture [6].

Finally we remark that it is not immediately clear how to extend our results to estimate the number of elements in (3) when $k > 2$. We discuss this briefly at the end of Section 3, where we also pose an open question of independent interest.

Acknowledgements: We would like to thank our advisor Jeffrey Vaaler for several discussions which influenced the direction of our research on this problem, and for pointing out the formula (2).

2. THE GROUP RING OF \mathbb{Q}/\mathbb{Z}

Our proof of Theorem 2 depends on the following two elementary lemmas.

Lemma 1. *If q and r are relatively prime positive integers then*

$$F_q \times F_r = F_{qr}.$$

Proof. By our definitions we have that

$$(5) \quad F_q \times F_r = \sum_{\substack{a=1 \\ (a,q)=1}}^q \sum_{\substack{b=1 \\ (b,r)=1}}^r z^{(ar+bq)/qr}.$$

If $c \in \mathbb{Z}$, $(c, qr) = 1$ then the equation

$$ar + bq = c$$

has a unique solution $(a, b) \in (\mathbb{Z}/q)^* \times (\mathbb{Z}/r)^*$. Conversely for any integers a and b with $(a, q) = (b, r) = 1$ we have that $(ar + bq, qr) = 1$. Thus the map $(a, b) \mapsto ar + bq$ is a bijection from $(\mathbb{Z}/q)^* \times (\mathbb{Z}/r)^*$ onto $(\mathbb{Z}/qr)^*$. Comparing this with (5) now finishes the proof. \square

Lemma 2. *Let p be prime and let $\alpha, \beta \in \mathbb{Z}$, $1 \leq \alpha \leq \beta$. Then we have that*

$$F_{p^\alpha} \times F_{p^\beta} = \begin{cases} \varphi(p^\alpha) F_{p^\beta} & \text{if } \alpha < \beta, \text{ and} \\ \varphi(p^\alpha) \sum_{i=0}^{\alpha-1} F_{p^i} - p^{\alpha-1} F_{p^\alpha} & \text{if } \alpha = \beta. \end{cases}$$

Proof. First let us prove the case when $\alpha = \beta$. We have that

$$(6) \quad F_{p^\alpha} \times F_{p^\alpha} = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^\alpha} \sum_{\substack{b=1 \\ (b,p)=1}}^{p^\alpha} z^{(a+b)/p^\alpha}.$$

If a is any integer with $(a, p) = 1$ then working in \mathbb{Z}/p^α we have that

$$(7) \quad \{a + b \mid b \in (\mathbb{Z}/p^\alpha)^*\} = (\mathbb{Z}/p^\alpha) \setminus \{a + np \pmod{p^\alpha} \mid 0 \leq n < p^{\alpha-1}\}.$$

If a' is another integer with $(a', p) = 1$ and $a \not\equiv a' \pmod{p}$ then it is clear that

$$a + np \not\equiv a' + np \pmod{p^\alpha}$$

for any $0 \leq n < p^{\alpha-1}$. Furthermore if n and n' are two integers with $0 \leq n < n' < p^{\alpha-1}$ then we also have that

$$a + np \not\equiv a + n'p \pmod{p^\alpha}.$$

These comments reveal that for any integer m

$$\left| \bigcup_{a=mp+1}^{(m+1)p-1} \{a + np \pmod{p^\alpha} \mid 0 \leq n < p^{\alpha-1}\} \right| = (p-1)p^{\alpha-1}.$$

Since $|(\mathbb{Z}/p^\alpha)^*| = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$ this implies that

$$\bigcup_{a=mp+1}^{(m+1)p-1} \{a + np \pmod{p^\alpha} \mid 0 \leq n < p^{\alpha-1}\} = (\mathbb{Z}/p^\alpha)^*.$$

Combining this with (6) and (7) we find that

$$\begin{aligned} F_{p^\alpha} \times F_{p^\alpha} &= \varphi(p^\alpha) \sum_{c=1}^{p^\alpha} z^{c/p^\alpha} - p^{\alpha-1} F_{p^\alpha} \\ &= \varphi(p^\alpha) \sum_{i=0}^{\alpha} \sum_{\substack{c=1 \\ p^i \parallel c}}^{p^\alpha} z^{c/p^\alpha} - p^{\alpha-1} F_{p^\alpha} \\ &= \varphi(p^\alpha) \sum_{i=0}^{\alpha} \sum_{\substack{d=1 \\ (d,p)=1}}^{p^{\alpha-i}} z^{d/p^{\alpha-i}} - p^{\alpha-1} F_{p^\alpha} \\ &= \varphi(p^\alpha) \sum_{i=0}^{\alpha} F_{p^i} - p^{\alpha-1} F_{p^\alpha}, \end{aligned}$$

and this is exactly what we were trying to show.

Now let us consider the easier case when $\alpha < \beta$. First observe that

$$(8) \quad F_{p^\alpha} \times F_{p^\beta} = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^\alpha} \sum_{\substack{b=1 \\ (b,p)=1}}^{p^\beta} z^{(ap^{\beta-\alpha}+b)/p^\beta}.$$

For each integer $a \in (\mathbb{Z}/p^\alpha)^*$ we have that

$$\{ap^{\beta-\alpha} + b \pmod{p^\beta} \mid b \in (\mathbb{Z}/p^\beta)^*\} = (\mathbb{Z}/p^\beta)^*,$$

and using this fact in (8) yields the desired result. \square

Now we proceed to the proof of Theorem 2. The idea is simply to split the factorizations of q and r into pieces that we will then recombine using Lemmas 1 and 2.

Proof of Theorem 2. Let q_1, q_d, r_1 , and r_d be the unique positive integers which satisfy

$$\begin{aligned} q &= q_1 q_d d, \quad r = r_1 r_d d, \\ (q_1, d) &= (r_1, d) = 1, \quad \text{and} \\ p \mid q_d \text{ or } r_d \text{ and } p \text{ prime} &\Rightarrow p \mid d, \end{aligned}$$

and let $d_{qr} = d/d'$. It follows immediately that $(d', q_d r_d) = 1$. Since d' is the largest divisor of d with $(q/d, d') = (r/d, d') = 1$ it also follows that if p is prime and $p \mid d_{qr}$ then $p \mid q_d r_d$. This implies that $(d_{qr}, d') = 1$. By Lemma 1 we have that

$$\begin{aligned} F_q \times F_r &= (F_{q_1} \times F_{q_d d_{qr}} \times F_{d'}) \times (F_{r_1} \times F_{r_d d_{qr}} \times F_{d'}) \\ (9) \quad &= F_{q_1 r_1} \times (F_{q_d d_{qr}} \times F_{r_d d_{qr}}) \times (F_{d'} \times F_{d'}). \end{aligned}$$

Now $(q/d, r/d) = 1$ so we can find distinct primes $p_1, \dots, p_\ell, p_{\ell+1}, \dots, p_k$ and positive integers a_1, \dots, a_k for which

$$\begin{aligned} q_d &= p_1^{a_1} \cdots p_\ell^{a_\ell}, \quad \text{and} \\ r_d &= p_{\ell+1}^{a_{\ell+1}} \cdots p_k^{a_k}. \end{aligned}$$

By our comments above there must also be positive integers b_1, \dots, b_k for which

$$d_{qr} = p_1^{b_1} \cdots p_k^{b_k}.$$

Now writing

$$\begin{aligned} q_d d_{qr} &= p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \text{and} \\ r_d d_{qr} &= p_1^{\beta_1} \cdots p_k^{\beta_k} \end{aligned}$$

we find that $\alpha_i, \beta_i \in \mathbb{Z}^+$ and that $\alpha_i \neq \beta_i$ for each $1 \leq i \leq k$. By Lemma 2 this implies that

$$F_{p_i^{\alpha_i}} \times F_{p_i^{\beta_i}} = \begin{cases} \varphi(p_i^{\alpha_i}) F_{p_i^{\beta_i}} & \text{if } 1 \leq i \leq \ell, \quad \text{and} \\ \varphi(p_i^{\beta_i}) F_{p_i^{\alpha_i}} & \text{if } \ell < i \leq k. \end{cases}$$

Applying Lemma 1 then yields

$$\begin{aligned} F_{q_d d_{qr}} \times F_{r_d d_{qr}} &= \prod_{i=1}^k \left(\varphi \left(p_i^{\min\{\alpha_i, \beta_i\}} \right) F_{p_i^{\max\{\alpha_i, \beta_i\}}} \right) \\ &= \varphi(d_{qr}) F_{q_d r_d d_{qr}}. \end{aligned}$$

Since

$$\varphi(p^\alpha) - p^{\alpha-1} = \varphi(p^\alpha) \frac{p-2}{p-1},$$

another application of Lemmas 1 and 2 gives us

$$\begin{aligned} F_{d'} \times F_{d'} &= \prod_{p^\alpha \parallel d'} \left(\varphi(p^\alpha) \sum_{i=0}^{\alpha} c(d', d'/p^i) F_{p^i} \right) \\ &= \varphi(d') \sum_{e \mid d'} c(d', d'/e) F_e \end{aligned}$$

$$= \varphi(d') \sum_{e|d'} c(d', e) F_{d'/e}.$$

Note that here we are also using the fact that $c(d', d'/e)$ is a multiplicative function of e . Returning to equation (9) we now have that

$$\begin{aligned} F_q \times F_r &= F_{q_1 r_1} \times \varphi(d_{qr}) F_{q_d r_d d_{qr}} \times \varphi(d') \sum_{e|d'} c(d', e) F_{d'/e} \\ &= \varphi(d) \sum_{e|d'} c(d', e) F_{q_1 r_1 q_d r_d d_{qr} d'/e} \\ &= \varphi(d) \sum_{e|d'} c(d', e) F_{qr/de}, \end{aligned}$$

which finishes the proof of Theorem 2. \square

The assertions of Corollaries 1 and 2 follow readily from the Theorem. We leave the proofs to the reader.

3. THE CARDINALITY OF $\mathcal{F}_Q + \mathcal{F}_Q$

In this section we will prove Theorem 1. We begin by writing

$$I_Q = |\mathcal{F}_Q + \mathcal{F}_Q|,$$

and by defining an arithmetical function

$$\tau_Q^*(n) = \sum_{\substack{d|n \\ d, n/d \leq Q \\ (d, n/d)=1}} 1.$$

By appealing to Corollary 2 we have that

$$I_Q = \sum_{\substack{n \leq Q^2 \\ \tau_Q^*(n) \geq 1}} \varphi(n).$$

A trivial upper bound for this quantity is given by

$$I_Q \leq Q^2 \cdot |\{n \leq Q^2 : \tau_Q^*(n) \geq 1\}|.$$

Estimating the cardinality of the set of integers which appears here is closely related to the “multiplication table problem” posed by Erdős ([2],[3]). This problem is solved in [5], where it is proved that the number of integers less than or equal to Q^2 which can be written as a product of two positive integers $n, m \leq Q$ is

$$O\left(\frac{Q^2}{(\log Q)^\delta (\log \log Q)^{3/2}}\right),$$

where $\delta = 1 - (1 + \log \log 2)/\log 2$. This immediately gives us the upper bound in Theorem 1. The lower bound is much more delicate and to deal with it we will closely follow ideas developed by K. Ford. For each $a \in \mathbb{N}$ we define $\mathcal{L}(a) \subset \mathbb{R}$ by

$$\mathcal{L}(a) = \bigcup_{d|a} [\log d - \log 2, \log d).$$

Roughly speaking, the Lebesgue measure of $\mathcal{L}(a)$ measures the clustering of the divisors of a . Our proof will rest crucially on the following estimate.

Lemma 3. *With $\mathcal{L}(a)$ defined as above we have as $Q \rightarrow \infty$ that*

$$(10) \quad \sum_{\substack{a \leq Q \\ \mu(a) \neq 0}} \frac{\varphi(a)|\mathcal{L}(a)|}{a^2} \gg \frac{(\log Q)^{2-\delta}}{(\log \log Q)^{3/2}},$$

where δ is the same as in Theorem 1 and $|\mathcal{L}(a)|$ denotes Lebesgue measure.

A similar bound, without the factor of $\varphi(a)/a$ in the summand, is proved in Section 2 of [5]. The proof there uses a clever application of the cycle lemma from combinatorics. The presence of the factor $\varphi(a)/a$ in our sum adds only minor difficulties. In fact all changes which arise by this modification are overcome by the multiplicativity of the function $\varphi(a)/a$, together with the fact that the sequences of integers under consideration are well distributed. Instead of giving a lengthy proof of our own, we leave this as a matter of fact for the reader to check.

Now if $n \in \mathbb{N}$ and $y, z \in \mathbb{R}$ then let $\tau(n; y, z)$ denote the number of divisors of n lying in the interval $(y, z]$. We will obtain our lower bound by considering only special types of integers in the sum I_Q . First note that

$$(11) \quad I_Q \geq \sum_{\substack{n \leq \frac{Q^2}{2} \\ \tau(n; Q/2, Q) \geq 1 \\ \mu(n) \neq 0}} \varphi(n),$$

since if $d|n$, $d > Q/2$, and n is square-free, then we must have that $n/d < Q$ and $(d, n/d) = 1$. Next write $y = y(Q) = Q/2$ and $x = x(Q) = Q^2/2$, and define \mathcal{A}_Q to be the set of square-free integers $n \leq x$ which can be factored in the form $n = apq$ with $1 \leq a \leq y^{1/8}$, p a prime such that $\log(y/p) \in \mathcal{L}(a)$, and $q > y^{1/8}$ is a prime. For reference we display this definition as

$$\mathcal{A}_Q = \left\{ n = apq \leq x : \mu(n) = 0, a \leq y^{1/8} < q, \log(y/p) \in \mathcal{L}(a) \right\}.$$

If $n = apq \in \mathcal{A}_Q$ then working from the definition of $\mathcal{L}(a)$ we see that p lies in an interval of the form $(y/d, 2y/d]$ for some $d|a$. Thus we have that $y^{7/8} \leq p \leq 2y$, and this shows that there can be at most two representations of n of the form which qualify it as an element of \mathcal{A}_Q (another one could possibly come from interchanging the roles of p and q). Furthermore we have that $dp \in (y, 2y]$, so $\tau(n; y, 2y) \geq 1$ and comparing with (11) we find that

$$(12) \quad I_Q \geq \sum_{n \in \mathcal{A}_Q} \varphi(n) \geq \frac{1}{2} \sum_{\substack{a \leq y^{1/8} \\ \mu(a) \neq 0}} \varphi(a) \sum_{\log(y/p) \in \mathcal{L}(a)} (p-1) I'_Q(a, p),$$

where

$$I'_Q(a, p) = \sum_{\substack{y^{1/8} < q \leq x/ap \\ (q, p) = 1 \\ q \text{ prime}}} (q-1).$$

For a lower estimate of I'_Q we employ the Prime Number Theorem to obtain

$$I'_Q(a, p) \gg \frac{\left(\frac{x}{ap}\right)^2}{\log \frac{x}{ap}} - \frac{y^{1/4}}{(\log y^{1/8})}.$$

Since $y^{7/8} \leq x/ap \leq 2y^{9/8}$ we have that $\log \frac{x}{ap} \ll \log y$ and that

$$I'_Q(a, p) \gg \frac{x^2}{a^2 p^2 \log y}.$$

Substituting this back into (12) gives us

$$(13) \quad I_Q \gg \frac{x^2}{\log y} \sum_{\substack{a \leq y^{\frac{1}{8}} \\ \mu(a) \neq 0}} \frac{\varphi(a)}{a^2} \sum_{\log(y/p) \in \mathcal{L}(a)} \frac{p-1}{p^2}.$$

Estimating the inner sum here is not difficult. First we divide the set $\mathcal{L}(a)$ into connected components. Each of these components has the form $[\log d - \log c, \log d]$ for some $d|a$ and $c \geq 2$. Thus we have that

$$\begin{aligned} \sum_{\log(y/p) \in [\log(d/c), \log d]} \frac{1}{p} &= \sum_{p \in (y/d, yc/d]} \frac{1}{p} \\ &= \log(\log(yc/d)) - \log(\log(y/d)) + O\left(\exp(-c_1 \sqrt{\log x})\right), \end{aligned}$$

where $c_1 > 0$ is a positive constant coming from the error term in the Prime Number Theorem. With a little manipulation it is not difficult to see that the latter expression is

$$\frac{\log c}{\log(y/d)} + O\left(\frac{1}{(\log Q)^2}\right) \gg \frac{\log c}{\log Q}.$$

Returning to (13) we now have that

$$I_Q \gg \frac{Q^4}{(\log Q)^2} \sum_{\substack{a \leq y^{\frac{1}{8}} \\ \mu(a) \neq 0}} \frac{\varphi(a) |\mathcal{L}(a)|}{a^2},$$

and combining this with (10) finishes the proof of our lower bound and of Theorem 1.

As we mentioned in the Introduction, it is an open problem to determine the order of magnitude of the cardinality of (3) when $k \geq 3$. The techniques used here would require some serious modifications to deal with those cases. Let us write $I_Q(k)$ for the cardinality of the sets in question. It follows from equation (1) and Corollary 2 that for $k \geq \pi(Q)$ we have that

$$I_Q(k) = |G_Q|.$$

We leave the reader with the following question. How small may we take k (as a function of Q) and still conclude that

$$\log I_Q(k) \asymp \log |G_Q|?$$

This seems to be an interesting problem which may possibly be solved by techniques that differ from those used here.

REFERENCES

- [1] C. Cobeli and K. Ford and A. Zaharescu, The jumping champions of the Farey series, *Acta Arith.* 110 (2003), no.3, 259-274.
- [2] P. Erdős, Some remarks on number theory, *Riveon Lematematika* 9 (1955), 45-48, (Hebrew. English summary).

- [3] P. Erdős, An asymptotic inequality in the theory of numbers, *Vestnik Leningrad. Univ.* 15 (1960), no. 13, 41-49, (Russian).
- [4] K. Ford, The distribution of integers with a divisor in a given interval, *Ann. of Math.* (2008), to appear.
- [5] K. Ford, Integers with a divisor in $(y, 2y]$, proceedings of *Anatomy of Integers* (Montreal, March 2006), to appear.
- [6] G. Harman, *Metric Number Theory* London Mathematical Society Monographs. New Series, 18. The Clarendon Press, Oxford University Press, New York, 1998.
- [7] A. Haynes, Notes on overlap estimates, preprint, <http://people.brandeis.edu/~akh/>.
- [8] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, 105, Cambridge University Press, Cambridge, UK, 2006.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF YORK, HESLINGTON, YORK YO10 5DD, UK
E-mail address: `akh502@york.ac.uk`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS, AUSTIN, TEXAS 78712, USA
E-mail address: `khomma@math.utexas.edu`